

V. Giovannetti, S. Lloyd*, and L. Maccone.

*Massachusetts Institute of Technology, Research Laboratory of Electronics***Corresponding Author: Department of Mechanical Engineering MIT 3-160,
Cambridge, MA 02139, USA.*

(July 30, 2001)

Abstract. A method is proposed to employ entangled and squeezed light for determining the position of a party. An accuracy gain over analogous protocols that employ classical light of equal spectrum is demonstrated. A similar procedure may be employed to enhance the accuracy when synchronizing clocks of distant parties. It is shown how the accuracy increase scales with the system resources and how it compares with analogous, but unentangled, protocols. The presence of a lossy channel and imperfect photodetection is considered. The advantages in using partially entangled states is discussed. A quantum cryptographic positioning scheme is given, which allows only trusted parties to learn the position of whatever must be localized.

From the realm of thought experiments, quantum entanglement has recently become exploitable for various applications and almost ready for technological implementations in fields such as quantum cryptography [1]. Other applications for entanglement and squeezing have been proposed in fields such as interferometric measurements [2], frequency measurements [3], lithography [4], algorithms [5], *etc.* In this paper a recent proposal [6] to exploit entanglement and squeezing to enhance the accuracy of position measurements and clock synchronization is thoroughly analyzed.

In Sect. I the proposal of [6] is briefly reviewed and the notation that will be employed is presented. The positioning protocol is derived and compared to similar, but unentangled, procedures to show the enhancement obtainable. In particular, the role of the entanglement and of the squeezing are separately analyzed in Subsects. IB and IC. The clock synchronization protocol is also described. In Sect. II the analysis of the protocol is given in the presence of loss, by considering the possibility that some photons are lost through dissipative processes during their travel or at the detection stage. The loss of a single photon in the maximally entangled state makes the resulting state completely useless. On the other hand, the loss of a photon in the unentangled case is not so dramatic since information on the time of arrival of the pulse may still be obtained by measuring the times of arrival of the remaining photons. However, by comparing the time of arrival information that can be obtained in the two cases, one sees that one still does better by using entangled states in a wide range of cases. The robustness to

loss stems from the fact that the accuracy gain obtained through entanglement is high enough to beat the classical (unentangled case) accuracy even when some time of arrival data must be discarded. In Sect. III, the assumption of using maximally entangled states is relaxed. There is a trade-off between the degree of entanglement (or the accuracy gain) and the robustness to noise. A higher robustness against loss ensues by decreasing the degree of entanglement, at the cost of reducing the accuracy gain achievable. Given the loss of the available channel, one will have to optimize the states to be employed. A scheme which is analogous to fault tolerant quantum computation is presented. It is possible to protect, at least partially, the entanglement from the loss by devising entangled states where the loss of one or more photons allows some information to be retained from the photons which do arrive. An example of such states is derived in detail. In Sect. IV two different cryptographic schemes that apply to the proposed protocol are derived. The first is essentially a classical protocol, but allows an accuracy enhancement over the unentangled case. The second is a quantum cryptographic scheme derived from the BB84 protocol [1]. Employing the latter procedure, any trusted party may be allowed to learn the position of whatever he must localize without anyone else discovering it.

I. POSITIONING ENHANCEMENT THROUGH ENTANGLEMENT

In this section a brief review of the method proposed in [6] is given. The positioning problem is defined and the formalism that will be used in the rest of the paper is laid out. First the case of classical states is explained. The enhancement in the positioning obtained by using entangled-squeezed states is then given and analyzed, by comparing it to what one would obtain with classical states of equal spectral characteristics.

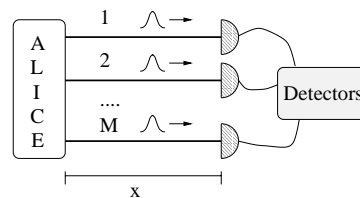


FIG. 1. Idealized experimental situation: Alice sends M light pulses to position is obtained by averaging the times of arrival t_i of the pulses she

For the sake of simplicity, consider the case in which one party (say Alice) wants to measure her distance from the detectors' position x by sending a light pulse to each of the M detectors which are placed in a known position (refer to Fig. 1). This situation can be easily generalized to different situations, such as the case in which the detectors are not all in the same position, the case in which less than M detectors are used by sending M time-separated pulses, *etc.* Since each dimension is to be treated independently, the analysis is limited to the one-dimensional case only. In the case depicted in Fig. 1, Alice's position is obviously given by

$$x = \frac{1}{M} \sum_{i=1}^M ct_i \equiv c \langle t \rangle, \quad (1)$$

where t_i is the travel time of the i -th pulse and c is its speed. Given the spectral characteristics of each pulse, its time of arrival t_i will have an intrinsic indetermination, *e.g.* for a Gaussian pulse with frequency spread $\Delta\omega$, one would have an error $\Delta t \propto 1/\Delta\omega$ in the time of arrival measurement. One can do better by measuring the rise time of the pulse or some other pulse characteristic that might be evaluated more accurately. Anyhow the unsurpassable limit for classical measurements is given by the shot noise limit: one must at least measure a single photon. From central limit theorem considerations, it follows that even if single photons are detected, in a pulse with N average photons the error in the time of arrival measurement is given by $\Delta t \propto 1/(\Delta\omega\sqrt{N})$. Thus, if Alice uses M Gaussian pulses of equal frequency spread $\Delta\omega$, the indetermination in the measurement of x , through Eq. (1), is $\Delta x \propto c/(\sqrt{MN}\Delta\omega)$. In the case of generic shaped pulses, starting from the pulse state, one must evaluate the mean value $\langle t \rangle$ for the x measurement and the variance Δt^2 for its accuracy. The considerations based on the central limit theorem do not always apply if quantum mechanics is taken into account. In fact, entanglement and squeezing allow one to correlate the time of arrival of different photons and to reduce the uncertainty on the measurement of $\langle t \rangle$. As will be shown, this allows an accuracy enhancement by a quantity \sqrt{MN} over the classical case.

Before the results are derived, the formalism is now introduced. The probability to detect a photon at time t and at position x in an ideal photodetector with infinite time resolution is given by the Glauber-Mandel formula [7,8]

$$P(t) \propto \left\langle E^{(-)}(t - x/c) E^{(+)}(t - x/c) \right\rangle, \quad (2)$$

where the ensemble average is the expectation on the quantum state of the radiation. All actual photodetectors are of course non-ideal, but the fundamental limit to the error introduced by the non-ideal features of photodetectors is given by the bandwidth of the photodetector rather than the bandwidth of the detected photon [9]. In

addition, this error can in principle be made as small as desired by devoting more resources (of energy, power, etc.) to the photodetection process. For M different communication channels, each of which may receive more than one photon, Eq. (2) generalizes to

$$P_M(t_{i,k}; N_i) \propto \left\langle : \prod_{i=1}^M \prod_{k=1}^{N_i} E_i^{(-)}(t_{i,k}) E_i^{(+)}(t_{i,k}) : \right\rangle, \quad (3)$$

where $t_{i,k}$ is the time of arrival of the k -th photon in the i -th channel, N_i is the number of photons detected in the i -th channel, and the detection time is shifted by the detector's position x_i : $t_{i,k} \rightarrow t_{i,k} + x_i/c$. In Eq. (3), the signal field at time t is given by

$$E_i^{(-)}(t) \equiv \int d\omega a_i^\dagger(\omega) e^{i\omega t}; \quad E_i^{(+)} \equiv \left(E_i^{(-)}\right)^\dagger, \quad (4)$$

where $a_i(\omega)$ is the field annihilator of a quantum of frequency ω at the i -th detector position. In the continuous Fock space formalism [10] of Eq. (4), the field annihilation operator is not dimensionless and satisfies the commutation relation

$$[a_i(\omega), a_j^\dagger(\omega')] = \delta_{ij} \delta(\omega - \omega'), \quad (5)$$

where the Kronecker delta accounts for the independence of the channels. The electromagnetic field has been quantized so that $E^{(-)}E^{(+)}$ is given in units of photons per second. The probability $P_M(t_{i,k}; N_i)$ must be normalized so that, when integrated over all the arrival times $t_{i,k}$, it gives the probability of detecting N_i photons in the i -th channel. In the case of unit quantum efficiency $\eta = 1$, this is also the probability of having N_i photons in the channel. In the case $\eta < 1$ this is not true anymore, because there is a probability $1 - \eta$ that a photon will be lost in the channel or at the photodetection stage. A detailed analysis of this case is given in Sect. II. In the cases of coherent states and of states with definite number of photons that will be considered here, this choice of normalization allows to use the formula (3) instead of the more complicated conditional joint probability (see [8] Chap. 14.8) of measuring *only* N_i photons at times $t_{i,k}$ and no more in each of the M channels.

Consider the situation depicted in Fig. 1, where all the detectors are placed at the same position x . The probability $P_M(t_{i,k}; N_i)$ of Eq. (3) contains all the timing information relative to the transmitted pulses sent by Alice. In particular, the average time of arrival $\langle t \rangle$ needed for the position measurement through Eq. (1) can be obtained by taking the average of the quantity

$$T \equiv \frac{1}{M} \sum_{i=1}^M \frac{1}{N_i} \sum_{k=1}^{N_i} t_{i,k} \quad (6)$$

over the probability $P_M(t_{i,k}; N_i)$, namely

$$\langle t \rangle = \sum_{N_i} \int dt_{i,k} P_M(t_{i,k}; N_i) T, \quad (7)$$

where the sum is performed on the values of N_i for all i and the integration is performed on all the $t_{i,k}$. The statistical error in determining $\langle t \rangle$ from the measurement results is given by the variance of T . In the following subsections the enhancement in accuracy obtainable by using entanglement and squeezing over classical states is derived by comparing how this variance changes from the classical to the quantum case. In particular, in subsection IA, the generic entangled-squeezed case is analyzed. In subsection IB, only the role of the entanglement is addressed, while in subsection IC, the role of squeezing is emphasized. In Sect. I of this paper, the analysis is limited to the case of unit quantum efficiency $\eta = 1$.

A. Entangled-squeezed vs. classical

The M coherent pulses a “classical” Alice would send to the reference detectors are described by a state of the radiation field of the form

$$|\Psi\rangle_{cl} = \bigotimes_{i=1}^M \bigotimes_{\omega} |\alpha[\phi(\omega)\sqrt{N}]\rangle_i, \quad (8)$$

where ω is the pulses carrier frequency, $\phi(\omega)$ is their spectral function, $|\alpha[\lambda(\omega)]\rangle_i$ is a coherent state of frequency ω and amplitude $\lambda(\omega)$ directed towards the i -th detector, and N is the mean number of photons in each pulse. The pulse spectrum $|\phi(\omega)|^2$ has been normalized so that $\int d\omega |\phi(\omega)|^2 = 1$. Upon calculating the ensemble average of Eq. (3) with the state $|\Psi\rangle_{cl}$ using the property

$$a(\omega') \bigotimes_{\omega} |\alpha[\lambda(\omega)]\rangle = \lambda(\omega') \bigotimes_{\omega} |\alpha[\lambda(\omega)]\rangle, \quad (9)$$

one obtains the probability density

$$P_M(t_{i,k}; N_i) \propto \prod_{i=1}^M \prod_{k=1}^{N_i} |g(t_{i,k})|^2, \quad (10)$$

where $g(t)$ is the Fourier transform of the spectral function $\phi(\omega)$:

$$g(t) = \frac{1}{\sqrt{2\pi}} \int d\omega \phi(\omega) e^{-i\omega t}. \quad (11)$$

Notice that the probability P_M factorizes, since in the classical state all the photons are independent. The quantity $|g(t_{i,k})|^2$ is the probability that the k -th photon is received on the i -th channel at time $t_{i,k}$. Define $\Delta\tau^2$ as the variance of $|g(t_{i,k})|^2$ (which is independent on i and k since all the photons have the same spectrum). From Eq. (10) it follows that the statistical error relative to the mean time of arrival $\langle t \rangle$ is

$$\Delta t \gtrsim \frac{\Delta\tau}{\sqrt{MN}}, \quad (12)$$

with approximate equality for $N \gg 1$.

Now compare this result with the one obtained from an entangled-squeezed state. Define number squeezed state of frequency ω the state $|N_\omega\rangle$ in which all modes are in the vacuum state, except for the mode at frequency ω which is populated by exactly N photons. The entangled-squeezed state that allows to achieve the most enhancement over the classical case is given by

$$|\Psi\rangle_{NM} = \int d\omega \phi(\omega) |N_\omega\rangle_1 \cdots |N_\omega\rangle_M. \quad (13)$$

By choosing the same spectral function $\phi(\omega)$ of the state (8), the spectral characteristics of each of the channels of the state $|\Psi\rangle_{NM}$ (obtained by tracing $|\Psi\rangle_{NM}$ over all the other channels) is the same as the classical state. Notice that $|\Psi\rangle_{NM}$ is a frequency maximally entangled state: a measurement of the frequency of a single one of its photons will have a random outcome weighted by the probability $|\phi(\omega)|^2$, but will determine the frequency of all the other photons. Since the number of photons in each channel is fixed (N) and no photons are lost ($\eta = 1$), then the probability $P_M(t_{i,k}; N_i)$ is null for $N_i \neq N$, thanks to the chosen normalization discussed previously. For $N_i = N$, inserting $|\Psi\rangle_{NM}$ in Eq. (3), it follows

$$P_M(t_{i,k}; N) \propto |g(\sum_{i=1}^M \sum_{k=1}^N t_{i,k})|^2, \quad (14)$$

where the property $[a_i(\omega')]^N |N_\omega\rangle_j = \delta_{ij} \delta(\omega - \omega') \sqrt{N!} |0\rangle$ was employed ($|0\rangle$ being the normalized vacuum state) and $g(t)$ is the same of Eq. (11). Eq. (14) shows that the entanglement in frequency translates into the bunching of the times of arrival of the photons of different pulses: although their individual times of arrival are random, the average $T = \frac{1}{MN} \sum_{i,k} t_{i,k}$ of these times is highly peaked. Indeed, from Eq. (14) it results that the probability distribution of T is $|g(MNT)|^2$. This immediately implies that the average time of arrival is determined to an accuracy

$$\Delta t = \frac{\Delta\tau}{MN}, \quad (15)$$

where $\Delta\tau$ is the same of Eq. (12). This result shows a \sqrt{MN} accuracy improvement over the classical case (12). The Margolus-Levitin theorem implies that a \sqrt{MN} improvement in accuracy is the best that can be obtained [11].

Notice that when the state $|\Psi\rangle_{NM}$ is used, the results of the single time of arrival measurement are meaningless: it is necessary to make correlation measurements, *i.e.* in this case one must consider the *sum* of the times of arrival of all the photons as in the quantity T . This implies that the geometry of the problem that can be solved depends on the state that can be produced. The state $|\Psi\rangle_{NM}$, which is tailored as to give the least indetermination in the physical quantity T , is appropriate for

the geometry of the case given in Fig. 1, where the sum (1) of the pulses' time of arrival is needed. Other maximally entangled states have to be tailored for different geometric dispositions of the detectors [6].

In conclusion, the suggested positioning protocol requires: 1) to produce and deploy the maximally entangled state suited for the given disposition of the reference points; 2) to measure the time of arrival $t_{i,k}$ of k -th photon in the i -th reference point and 3) to collect and compare the results in order to have the needed correlation measurement. In practice, the correlation can be performed by using the bunching properties of the time of arrival measurements of frequency entangled pulses.

B. Entangled vs. unentangled

The results of subsection IA combined entanglement and squeezing to give the maximum quantum enhancement of positioning, in subsections IB and IC, the distinct and complementary rules of entanglement and squeezing will be elucidated. First, the general result of the previous subsection will be specialized to emphasize the role of the entanglement: a maximally entangled state is compared to a similar unentangled one.

Consider the frequency maximally entangled state of M photons defined by

$$|\Psi\rangle_{en} \propto \int d\omega \phi(\omega) |\omega\rangle_1 \cdots |\omega\rangle_M, \quad (16)$$

where $|\omega\rangle \equiv |1_\omega\rangle$ and the ket subscripts indicate the detector each mode is directed to. Specifying Eq. (14) to the case $N = 1$, one immediately finds

$$P_M(t_1, \dots, t_M) \propto |g(\sum_{i=1}^M t_i)|^2 \quad (17)$$

and thus the error in the evaluation of the average time of arrival $\langle t \rangle$ is given by

$$\Delta t = \frac{\Delta\tau}{M}. \quad (18)$$

This result must be compared to the results one would obtain using uncorrelated photons with the same spectral characteristics as the state $|\Psi\rangle_{en}$, *i.e.* the state defined as

$$|\Psi\rangle_{un} = \bigotimes_{i=1}^M \int d\omega_i \phi(\omega_i) |\omega_i\rangle_i, \quad (19)$$

which describes M uncorrelated single photon pulses each with spectral function $\phi(\omega)$. Each of these pulses has the same spectral characteristics as the photons in the entangled state $|\Psi\rangle_{en}$, as can be seen by looking at the spectrum of the state obtained by tracing away all but one of the modes in (16), *i.e.*

$$\text{Tr}_{M-1} [|\Psi\rangle_{en} \langle \Psi|] = \int d\omega |\phi(\omega)|^2 |\omega\rangle \langle \omega|, \quad (20)$$

where Tr_{M-1} indicates the trace over all M frequency modes except one. Using again Eq. (3) on the state $|\Psi\rangle_{un}$, one finds that

$$P_M(t_1, \dots, t_M) = \prod_{i=1}^M |g(t_i)|^2. \quad (21)$$

The variance of P_M on the times of arrival of the M photons gives the accuracy

$$\Delta t = \frac{\Delta\tau}{\sqrt{M}}, \quad (22)$$

where $\Delta\tau$ is the same as in Eq. (18). An increase in accuracy by \sqrt{M} is evident from the comparison of Eqs. (18) and (22). This shows that the \sqrt{M} increase obtained in the previous subsection for the general case is an effect of the entanglement between the channels present in the state $|\Psi\rangle_{NM}$.

The quantum states that are needed in order to implement the ideas presented here are difficult to obtain in practice. In fact, one requires entanglement of many pulses in the continuous degree of freedom of the frequency. An example for $M = 2$ of this kind of states is the cw pumped twin beam state at the output of a parametric downconversion [8], which to first order (ignoring the vacuum component) is given by

$$|\Psi\rangle_{tb} = \int d\omega \phi(\omega) |\omega\rangle_s |\omega_0 - \omega\rangle_i, \quad (23)$$

where ω_0 is the pump frequency and s and i refer to the signal and idler modes respectively. Notice that it is not exactly a state of the form (16) since it is anticorrelated in frequency: namely in (16) the difference in the frequency of the photons is fixed, while in (23) the sum is fixed. The anticorrelation allows to recover the difference in time of arrival [12,13], instead of the sum as in the case of $|\Psi\rangle_{en}$. Thus, the twin beam state may be employed in the cases where the difference in time of arrival is needed for position measurements, *i.e.* when the two detectors are in opposite directions with respect to Alice: one to her left and one to her right. By using the techniques of the two-photon laser [14], it seems that it could be possible to extend the entanglement of (23) at least to the case of 4 photons. In fact, if one seeds the two photon laser with a twin beam state of the form (23) one can obtain at the output a frequency entanglement on a bandwidth $\Delta\omega$ proportional to the indeterminacy of the virtual energy level needed for the lasing to occur.

This subsection is focused on the role of number squeezing. A comparison is made between an N photon number squeezed state and a coherent state of N average photons.

Consider the number squeezed state obtained from (13) for a single channel ($M = 1$), *i.e.*

$$|\Psi\rangle_N = \int d\omega \phi(\omega) |N_\omega\rangle. \quad (24)$$

From Eq. (15), it follows that the average of the photon times of arrival can be determined with an uncertainty of

$$\Delta t = \frac{\Delta\tau}{N}. \quad (25)$$

On the other hand, the single channel coherent pulse given by (8) for $M = 1$, yields

$$\Delta t \gtrsim \frac{\Delta\tau}{\sqrt{N}}. \quad (26)$$

Here an accuracy increase of \sqrt{N} is evident from the comparison of (25) and (26). This shows that the \sqrt{N} enhancement obtained in Subsect. IA has to be attributed to the number squeezing present in the state $|\Psi\rangle_{NM}$.

The similarity of the results obtained in Subsects. IB and IC stems from the fact that one can interpret the Fock state $|N_\omega\rangle$ as composed by N one-photon pulses entangled in frequency.

II. LOSS ANALYSIS IN THE IDEAL CASE

In this section the problem of the loss is addressed. The loss of a single photon from a maximally entangled state (such as $|\Psi\rangle_{MN}$) makes it completely useless for positioning, since the information is encoded in the entanglement and not on the single photons. On the other hand, the loss of a single photon from a “classical” state (such as $|\Psi\rangle_{cl}$ or $|\Psi\rangle_{un}$) allows still to recover information on the time of arrival of the remaining photons. Nonetheless, it will be shown that the gain in accuracy obtained by using entangled photons *vs.* unentangled is quite robust against the loss. In the first subsection the conditions on the channel quantum efficiency that is necessary to obtain an enhancement in the accuracy is derived. First a simple argument is given, then a more rigorous approach is discussed. In Subsect. IIB the effect of the loss on the state is studied in the density matrix formalism.

A. Condition on the quantum efficiency

One can understand the robustness to loss from the following intuitive explanation (the rigorous derivation

is given in detail later). For simplicity, initially consider the case of one photon per channel ($N = 1$). Given the channels’ quantum efficiency η (namely $1 - \eta$ is the probability that one photon is lost), then the probability that all M photons reach Alice is given by η^M . Repeating $r \gg 1$ times the whole experiment, a total number rM of photons is sent. In average only a fraction η^M of the experimental runs will not lose any photon. If Alice is employing the entangled states $|\Psi\rangle_{en}$ of Eq. (16) to evaluate the mean time of arrival $\langle t \rangle$, she must only use the data obtained from the experimental runs where all the M photons of the state reach the detectors. As will be shown, the other cases in which some of the photons are lost are useless. The evaluation of the time of arrival accuracy obtained from the r experimental runs through Eq. (18) will then be

$$\Delta t(r) = \frac{\Delta\tau}{M\sqrt{r\eta^M}}, \quad (27)$$

where the factor $1/\sqrt{r\eta^M}$ stems from the statistical independence of different experimental runs. On the other hand, if Alice employs r copies of the state $|\Psi\rangle_{un}$, all of the $\eta(rM)$ photons that in average reach the detectors may be employed to evaluate the time of arrival with an accuracy

$$\Delta t(r) \gtrsim \frac{\Delta\tau}{\sqrt{\eta r M}}, \quad (28)$$

where the equality holds for $rM \gg 1$. The condition for achieving a greater accuracy through the state $|\Psi\rangle_{en}$ than through $|\Psi\rangle_{un}$ is given by

$$\frac{\Delta\tau}{\sqrt{\eta r M}} > \frac{\Delta\tau}{M\sqrt{r\eta^M}} \implies \eta > \left(\frac{1}{M}\right)^{\frac{1}{M-1}}. \quad (29)$$

This condition is shown in Fig. 2. It is evident that relatively low values of quantum efficiency η are sufficient for obtaining the accuracy increase feature also for high numbers of entangled photons.

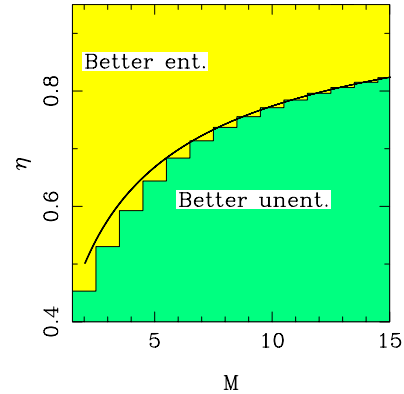


FIG. 2. Graph showing which values of quantum efficiency η are needed of M particles over the state $|\Psi\rangle_{un}$ of M particles. The higher region is where entangled state $|\Psi\rangle_{en}$ and the lower region is where a better accuracy is achieved through the condition (29). The histogram is obtained by the more rigorous approach for $M \gg 1$.

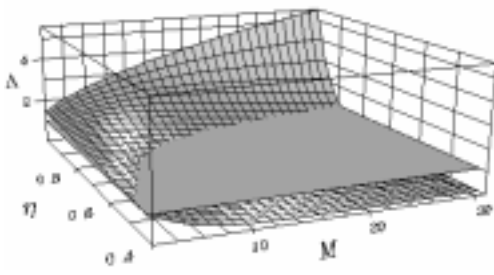


FIG. 3. Three dimensional graph depicting the gain in accuracy $\Lambda(M, \eta)$ vs. M and η . The horizontal plane in the figure for $\Lambda = 1$ separates the regions where it is better to employ $|\Psi\rangle_{en}$ (over) and $|\Psi\rangle_{un}$ (under). Notice the \sqrt{M} dependence for $\eta = 1$ which corresponds to the enhancement discussed in Subject. IB.

The intuitive reasoning that suggests the condition (29) must be taken only as a qualitative demonstration, since Eq. (28) is valid only for $M \gg 1$. Now the rigorous condition is derived. It turns out to be even more favorable to the entangled case, even though only a small correction to the condition (29) is required. Eq. (21) shows that, in the case of no loss, using an unentangled state $|\Psi\rangle_{un}$, the probability distribution $P_M(t_1, \dots, t_M)$ of the time of arrival of the M photons is just the product of the probability distributions of the times of arrival of the single photons $|g(t)|^2$. Thus, if each photon has a probability η of arriving and a probability $1 - \eta$ of being lost, then the probability of retaining m of the initial M photons is given by the binomial distribution

$$P_m(t_1, \dots, t_m) = \binom{M}{m} \frac{\eta^m (1 - \eta)^{M-m}}{1 - (1 - \eta)^M} \prod_{i=1}^M |g(t_i)|^2. \quad (30)$$

In this case, the integral of P_m over all the times of arrival t_1, \dots, t_m is the probability of retaining m of the M photons, but discarding the case in which all the photons are lost, an event that happens with probability $(1 - \eta)^M$. In fact, in the latter case no information on time of arrival is acquired and this is the source of the renormalization factor $1/[1 - (1 - \eta)^M]$ in Eq. (30). In particular for $\eta = 1$ Eq. (30) coincides with (21), namely $P_m(t_1, \dots, t_m) = 0$ for $m \neq M$. The accuracy that may be obtained from $|\Psi\rangle_{un}$ is given by the variance of the distribution given in (30), *i.e.*

$$\Delta t = \left[\sum_{m=1}^M \binom{M}{m} \frac{\eta^m (1 - \eta)^{M-m}}{m[1 - (1 - \eta)^M]^2} \right]^{\frac{1}{2}} \Delta \tau. \quad (31)$$

If the experiment is repeated $r \gg 1$ times, in a fraction $1 - (1 - \eta)^M$ of them at least one photon is received and the accuracy that can be reached in each of these cases is given by (31). Thus the overall accuracy for the r experiments is

$$\Delta t(r) = \left[\sum_{m=1}^M \binom{M}{m} \frac{\eta^m (1 - \eta)^{M-m}}{m[1 - (1 - \eta)^M]^2} \right]^{\frac{1}{2}} \frac{\Delta \tau}{\sqrt{r}}. \quad (32)$$

Again, by comparing this variance with the one obtained from the entangled case (27), one finds the condition un-

der which it is better to use entangled states with respect to unentangled ones, *i.e.*

$$\Lambda \equiv M \left[\sum_{m=1}^M \binom{M}{m} \frac{\eta^{M+m} (1 - \eta)^{M-m}}{m[1 - (1 - \eta)^M]^2} \right]^{\frac{1}{2}} > 1, \quad (33)$$

which for $M \gg 1$ coincides with condition (29). The condition (33) is plotted in Fig. 3.

B. Loss dynamical evolution

In this subsection the evolution of the states introduced previously is analyzed in the presence of loss.

It can be shown [15] that a lossy channel of quantum efficiency η (which also takes into account the detection efficiency) can be described by considering a perfect channel and inserting a beam splitter of transmissivity η . The second input port b of the beam splitter is in the vacuum state $|0\rangle$ and one output port is traced out (refer to Fig. 4).

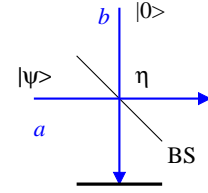


FIG. 4. Description of a lossy channel mode through a beam splitter efficiency.

This allows to obtain the non-unitary evolution of a lossy channel. It can be shown that, starting from the unitary evolution of the beam splitter

$$U = \exp \left[-\arctan \left(\sqrt{\frac{1 - \eta}{\eta}} \right) (ab^\dagger - a^\dagger b) \right] \quad (34)$$

(where the mode definition for a and b is given in Fig. 4), one obtains the following completely positive map for the density matrix evolution in the presence of loss

$$\varrho \longrightarrow \varrho' = \text{Tr}_b [U \varrho \otimes |0\rangle_b \langle 0| U^\dagger] = \sum_{n=0}^{\infty} V_n \varrho V_n^\dagger, \quad (35)$$

with

$$V_n = \left(\frac{1 - \eta}{\eta} \right)^{\frac{n}{2}} \frac{a^n}{\sqrt{n!}} \eta^{\frac{a^\dagger a}{2}}. \quad (36)$$

The case of frequency independent loss is considered. For each mode of the continuum of modes of the states given by (16) and (19), the evolution (35) must be calculated. In the case of the density operator $\varrho_{en} = |\Psi\rangle_{en} \langle \Psi|$ corresponding to the state (16), it is possible to show

$$\varrho'_{en} = \eta^M \varrho_{en} + \sum_{m=0}^{M-1} \eta^m (1-\eta)^{M-m} \times \int d\omega |\phi(\omega)|^2 \left[|\omega\rangle\langle\omega| \otimes |0\rangle\langle 0| \otimes \cdots + |0\rangle\langle 0| \otimes \cdots \right], \quad (37)$$

where $|0\rangle\langle 0|$ is the vacuum state and the term in square brackets is the sum of all the $\binom{M}{m}$ possible combinations of m times the state $|\omega\rangle\langle\omega|$ and $M-m$ times the vacuum $|0\rangle\langle 0|$. The interpretation of Eq. (37) is that none of the photons is lost and the state is unaffected with a probability η^M , and m photons are lost and the state is left in a mixture of $|\omega\rangle$ and $|0\rangle$ with probability $\binom{M}{m} \eta^m (1-\eta)^{M-m}$. Since the second term of the state (37) contains only density matrices diagonal in the $|\omega\rangle$ representation, it does not contain any information on the time of arrival measurement. In fact, the probability P_M defined in (3) gives a “constant” probability if applied to the state $|\omega\rangle\langle\omega|$. Thus post-selection measurements are needed in this case: if Alice is expecting the state $|\Psi\rangle_{en}$ given in (16), she must throw away all the data coming from events in which she recorded less than M photons. These events are useless. As shown before, the fragility to loss is only apparent, since the accuracy gain over the unentangled case is so high, that it is possible to find a wide experimental region in which the accuracy enhancement is preserved.

On the other hand, the evolution of the unentangled state of Eq. (19), $\varrho_{un} = |\Psi\rangle_{un}\langle\Psi|$, is given by

$$\varrho'_{un} = \sum_{m=0}^M \eta^m (1-\eta)^{M-m} \times \left[\varrho_1 \otimes \varrho_2 \otimes \cdots + |0\rangle\langle 0| \otimes \varrho_2 \otimes \cdots \right], \quad (38)$$

where the term in square brackets contains the sum of all possible combinations of m times the states ϱ_i and $M-m$ times the vacuum $|0\rangle\langle 0|$, and where

$$\varrho_i = \int d\omega d\omega' \phi(\omega) \phi^*(\omega') |\omega\rangle_i \langle\omega'|, \quad (39)$$

which is a single photon wavepacket with spectral function $\phi(\omega)$ in the i -th channel, *i.e.* the state (19) for $M=1$. Starting from the state in Eq. (38) no post-selection is necessary (except the obvious case in which Alice does not receive any photon), since all the terms are composed of the states of the form (39) which do retain time of arrival information.

The same analysis can be extended to the general case of the state $|\Psi\rangle_{NM}$, showing that the loss of a single photon destroys all the timing information. In fact, the same arguments given for $|\Psi\rangle_{en}$ apply also to the number squeezed state $|\Psi\rangle_N$ of Eq. (24). Its evolution is given by

$$\varrho'_N = \eta^N \varrho_N + \sum_{n=1}^N \binom{N}{n} \eta^n (1-\eta)^{N-n} \times \int d\omega |\phi(\omega)|^2 |n_\omega\rangle\langle n_\omega|, \quad (40)$$

where $\varrho_N = |\Psi\rangle_N \langle\Psi|$. Also here Alice has to throw away all the data she collects when she receives less than N photons: the state $|n_\omega\rangle\langle n_\omega|$ has no timing information.

III. TRADE-OFF ENTANGLEMENT VS. LOSS RESISTANCE

In this section some strategies for battling the effects of the loss are presented. Instead of using the maximally entangled states employed so far, one may devise strategies for using partially entangled states which turn out to be more robust to the loss. A simple example to illustrate this is first presented and a more sophisticated case is then analyzed in detail.

It is well known (see for example [16]) that when more than two systems are entangled, variety of different effects can occur. Hence, in order to address the relation occurring between the degree of entanglement of a state and its loss resistance, it is useful to start from a simple example. Consider the case depicted in Fig. 5, of one photon per channel ($N=1$) where the first Q of the M channels are maximally entangled as the ones in the state $|\Psi\rangle_{en}$ of Eq. (16) and the other $M-Q$ channels are unentangled as in $|\Psi\rangle_{un}$ of Eq. (19):

$$|\Psi\rangle_Q \propto \int d\omega \phi(\omega) |\omega\rangle_1 \cdots |\omega\rangle_Q \bigotimes_{i=Q+1}^M \int d\omega_i \phi(\omega_i) |\omega_i\rangle_i. \quad (41)$$

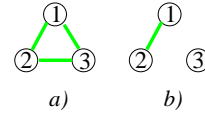


FIG. 5. Pictorial representation of the entanglement of three parties. The case *a*) is when the three parties are maximally entangled. The case *b*) is when only the first two parties are maximally entangled and the last is unentangled.

The parameter Q simply characterizes the degree of entanglement of $|\Psi\rangle_Q$: bigger values of Q correspond to higher entanglement. Consider first the case of unit quantum efficiency. As usual, using Eq. (3), the probability of the times of arrival is calculated as

$$P_M(t_1, \dots, t_M) \propto |g(\sum_{i=1}^Q t_i)|^2 \prod_{i=Q+1}^M |g(t_i)|^2. \quad (42)$$

The accuracy in the determination of $\langle t \rangle$ follows as

$$\Delta t = \frac{\Delta\tau}{\sqrt{M}} \sqrt{\frac{M-Q+1}{M}}. \quad (43)$$

For $Q > 1$ (*i.e.* at least two of the M channels are entangled), the accuracy achievable is greater than the completely unentangled case (22), but not as high as the completely entangled case (18). The loss of performance of this state is balanced by a greater resistance to the effects of photon losses than the maximally entangled state $|\Psi\rangle_{en}$. In fact, as shown in the previous section, the loss of a single photon renders the state $|\Psi\rangle_{en}$ completely useless for localization purposes. On the contrary, the loss of photons from $|\Psi\rangle_Q$ still allows to recover information, if a suitable post-selection is employed. Namely one must discard all the times of arrival of the entangled photons if one or more of them is lost, but all the times of arrival of the unentangled photons which do arrive can be safely retained. No information is obtained from $|\Psi\rangle_Q$ only when one or more of the entangled photons and also *all* the unentangled ones are lost. The loss of one of the unentangled photons of $|\Psi\rangle_Q$ reduces the accuracy only by a factor $\sqrt{\frac{M}{M-1}}$, and the loss of one (or more) of the entangled photons reduces the accuracy to the one obtainable by an unentangled state of $M - Q$ channels.

This simple example shows how one can increase the resistance to loss by reducing the entanglement, however at the cost of achieving less accuracy enhancement. Of course much more sophisticated configurations can be introduced for entangling multiple systems [16], in which the different systems share a different degree of entanglement with all the other systems. It is expected that also in the general case, a similar trade-off between the degree of entanglement and resilience to loss holds. Depending on the quantum efficiency of the channel and on the degree of entanglement one is able to produce, different strategies, involving different data processing or post-selections, are possible. A better insight on this may be gained by analyzing the following example, where a multi-structured entanglement is employed.

A procedure analogous to fault tolerant quantum computation may be introduced in our scheme. Consider again the simple case of one photon in each of the M channels ($N = 1$). Instead of sending the maximally entangled state $|\Psi\rangle_{en}$ of Eq. (16), Alice sends Bob a state in which groups of K photons are maximally entangled and $G = M/K$ groups are entangled together, as depicted in Fig. 6. If no photon is lost, then one will not only be able to use the correlations within all the groups, but also the correlation *between* the groups. In the event of a photon loss, thanks to the structure of the entanglement employed, not all the information will be lost as would happen when using the state $|\Psi\rangle_{en}$. In fact, suppose that the lost photon comes from the j -th group of photons: as will be shown, the only data that must be discarded is the data relative to the j -th group photon times of arrival. All the other times of arrival may be retained and employed. The procedure can also be nested, namely each of the G groups of K photons may be partitioned in maximally entangled subgroups and so on.

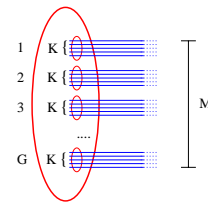


FIG. 6. Quantum fault tolerance applied to the quantum positioning problem (the state $|\Psi\rangle_G$ is frequency entangled) is composed of K frequency maximally entangled photons.

The state represented in Fig. 6 is given by

$$|\Psi\rangle_G \equiv \int d\Omega \Phi(\Omega) |\Omega\rangle_1 |\Omega\rangle_2 \cdots |\Omega\rangle_G, \quad (44)$$

where

$$|\Omega\rangle_j \equiv \int d\omega \phi(\omega, \Omega) |\omega\rangle_{j1} |\omega\rangle_{j2} \cdots |\omega\rangle_{jK} \quad (45)$$

is the state of the j -th group of K photons described by the one photon frequency state $|\omega\rangle_{jl}$ for $j = 1, \dots, G$ and $l = 1, \dots, K$. Consider for simplicity the case of Gaussian spectrum, namely $|\Phi(\Omega)|^2$ is a Gaussian with variance $\Delta\Omega^2$ and $|\phi(\omega, \Omega)|^2$ is a Gaussian centered around Ω with variance $\Delta\omega^2$. The state $|\Psi\rangle_{en}$ previously analyzed can be reobtained from $|\Psi\rangle_G$ in the limit $\Delta\omega \rightarrow 0$. Since $|\Omega\rangle_j$ has the same structure of $|\Psi\rangle_{en}$, if one photon is lost in the j -th group all the time of arrival information of such state must be discarded. Namely, only the g groups in which no photons have been lost can be still employed for the positioning. In this case, using the state $|\Psi\rangle_G$ in the ensemble average of Eq. (3) to calculate the probability density of detecting all the gK photons of the g groups at times $t_{j,l}$ is given by

$$P_{gK}(t_{j,l}) \propto \exp \left[- \left(\sum_{j=1}^g \sum_{l=1}^K t_{j,l} \right)^2 / (2\Delta\tau_g^2) \right], \quad (46)$$

where $t_{j,l}$ is the time of arrival of the l -th photon in the j -th group and

$$\Delta\tau_g = \frac{\sqrt{g}}{2\Delta\omega} \sqrt{\frac{(G-g)\Delta\Omega^2 + \Delta\omega^2}{G\Delta\Omega^2 + \Delta\omega^2}}. \quad (47)$$

Notice that Eq. (46) and (47) for $\Delta\omega \rightarrow 0$ and $G = g$ reproduce the result derived previously in (17) for Gaussian spectrum. Eq. (46) shows that even if $G - g$ groups are discarded because they lost some photons, the remaining g groups still retain some entanglement. In fact, since the $|\Omega\rangle_j$ are not orthogonal for $\Delta\omega > 0$, the probability $P_{gK}(t_{j,l})$ does not factorize in parts depending on the single groups. The proportionality constant in Eq. (46) must be chosen so that the integral of $P_{gK}(t_{j,l})$ over all the times gives the probability that only gK photons are detected, namely

$$P_g \equiv \binom{G}{g} \frac{(\eta^K)^g (1 - \eta^K)^{G-g}}{1 - (1 - \eta^K)^G}, \quad (48)$$

where η^K is the probability that all the photons of a group reach the detectors, and where, analogously as in Sect. II A, the term $1/[1 - (1 - \eta^K)^G]$ is introduced to take into account the case (to be discarded) in which all the G groups have lost at least one photon.

If g of the G groups do not lose any photon, one may estimate the mean time of arrival by calculating the mean value of $\sum_{j,l} t_{j,l}/(gK)$. The accuracy may be estimated by using the probability (46) obtaining

$$\Delta t = \frac{1}{2K\Delta\omega} \left[\sum_{g=1}^G \frac{(G-g)\Delta\Omega^2 + \Delta\omega^2}{g(G\Delta\Omega^2 + \Delta\omega^2)} \mathcal{P}_g \right]^{\frac{1}{2}}. \quad (49)$$

As before –see Eq. (32)– when $r \gg 1$ experimental runs are performed, the accuracy $\Delta t(r)$ that can be achieved is obtained from (49) by dividing Δt by the square root of the number of usable runs, namely $r[1 - (1 - \eta^K)^G]$.

In order to compare this result to what one would obtain in the unentangled case or in the maximally entangled case, one must employ the states $|\Psi\rangle_{en}$ and $|\Psi\rangle_{un}$ with the same single photon spectral characteristics of the photons of $|\Psi\rangle_G$. This can be achieved by using in $|\Psi\rangle_{en}$ and $|\Psi\rangle_{un}$ a Gaussian spectrum with variance $\Delta\omega^2 + \Delta\Omega^2$: namely, $\Delta\tau = 1/(2\sqrt{\Delta\omega^2 + \Delta\Omega^2})$. An example of the comparison between the performance of $|\Psi\rangle_{un}$ and $|\Psi\rangle_G$ when using such a coding scheme is given in Fig. 7, where the group-entangled state $|\Psi\rangle_G$ is shown to achieve a better accuracy than a non-entangled state $|\Psi\rangle_{un}$. Notice that the accuracy enhancement feature can be retained also for low quantum efficiency even when a high number M of particles is involved. A comparison between the accuracy enhancement obtainable with the states $|\Psi\rangle_{en}$, $|\Psi\rangle_{un}$ and $|\Psi\rangle_G$ is shown in Fig. 8.

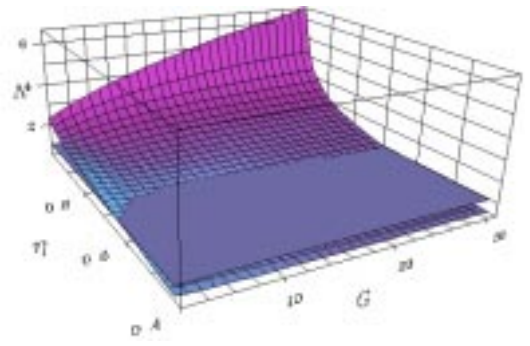
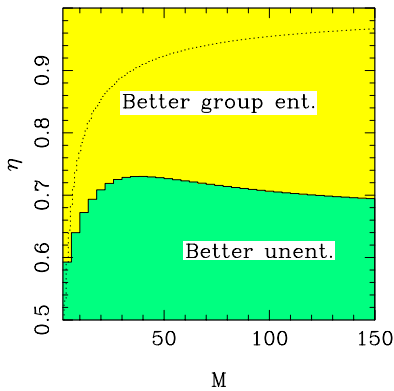


FIG. 7. Robustness to loss of the state (44). *Upper graph:* The upper plot shows the accuracy Δt by using the state $|\Psi\rangle_G$ (with $K = 4$ and $\Delta\omega^2/\Delta\Omega^2 = 2$) as compared to the unentangled case, which is the same as in Fig. 2 and shows the region where it is better to use maximally entangled states $|\Psi\rangle_{un}$. *Lower graph:* The same information as the previous graph is shown, but for the gain over the unentangled case.

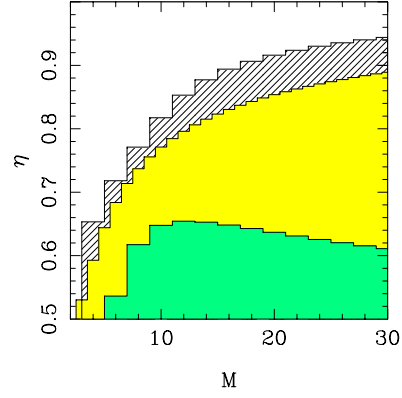


FIG. 8. The upper white region is where the maximally entangled state $|\Psi\rangle_G$ is better than the unentangled state $|\Psi\rangle_{un}$ (in the lower plot $G > en > un$; the light grey region is where $G > un > en$, and the dark grey region is where $en > G > un$ for this plot are $K = 2$ and $\Delta\omega^2/\Delta\Omega^2 = 2$.

IV. QUANTUM CRYPTOGRAPHIC POSITIONING

In this section two different cryptographic protocols will be given. The aim is for Alice to learn her position in space relative to Bob (located at the detectors position), without anybody else gaining *any* information by intercepting neither the photons nor the classical information Alice and Bob exchange. The first procedure is essentially a classical procedure and is roughly equivalent to performing the positioning using classical (unentangled) photons each of which has been delayed by an amount which is known only by Alice. In the quantum version given here, however, the accuracy for fixed number M of photons is increased over the classical version. This first protocol allows only Alice to recover her position: nobody else (including Bob) will be able to determine where she is. The second protocol is analogous to the quantum cryptographic key exchange BB84 [1] and will allow both Alice and Bob (and no one else) to recover her

position. It also is possible to modify this last protocol to include more complicated scenarios, such as the case in which also other trusted persons may be allowed to learn Alice's position, or (by suitably tailoring the entanglement of the exchanged pulses) the case in which some of the trusted persons may learn Alice's position *only* when they meet and exchange their data, or the case in which Alice herself is not allowed to discover her own position, *etc.*

Consider for simplicity the case of the state $|\Psi\rangle_{en}$. The extension to the general case $|\Psi\rangle_{NM}$ is straightforward. The first protocol is simply implemented by allowing Alice to detect the time of arrival of the photons in one of the M channels. She will send to Bob only the rest $M - 1$ photons. When Bob receives and measures them, he will use a public channel to broadcast the measurement result to Alice. As was shown in Sect. II, the loss of a single photon results in not being able to recover *any* information on Alice's position. Thus if an eavesdropper was to intercept the photons Alice sends Bob (the eavesdropper needn't even bother: he only has to wait for Bob's broadcast) he would obtain no information. Alice, on the other hand, simply has to add the random times of arrival that Bob tells her to the one she herself has measured. This allows her to find her position, with an uncertainty $\Delta t = \Delta\tau/(M - 1)$, since she only used $M - 1$ photons for the positioning. This protocol is roughly equivalent to a classical protocol in which Alice sends Bob photons she delayed each by a random amount of time she does not disclose. From Bob's random times of arrival she may recover her position without anybody else (including Bob) knowing it.

The second protocol allows both Alice and Bob to recover Alice's position without anybody else discovering it, but it can achieve only an increase in accuracy lower than the one found for the non-cryptographic positioning scheme. As before, Alice retains one photon and sends Bob the remaining $M - 1$. Thus, they share r copies of the state $|\Psi\rangle_{en}$ of which Alice has one photon and Bob has the remaining $M - 1$. For each of the r copies Alice and Bob choose randomly (and independently) to measure either the frequency or the time of arrival of *all* the photons. After that they compare which of the two observables they used on each of the r copies they exchanged: they discard all the cases in which the two observables do not match, namely Alice measured the frequency and Bob the time of arrival or *viceversa*. For all the cases in which both of them measured the frequency, they broadcast the measurement results. Since the state is maximally entangled in frequency, their measurement outcomes (though random) must agree. If this is not the case, they know that there is an eavesdropper which is ruining the states that are transiting between them. If all the frequency measurement outcomes do agree, they can be confident that no one is measuring the photon time of transit in the channel. Once they verified that no eavesdropper was present, Alice can broadcast the measurement results for half of the copies in which they both

measured the time of arrival and Bob can broadcast the measurement results of the other half. From the information they exchange, which is utterly useless for anybody else, both Alice and Bob may recover Alice's position. Of course an eavesdropper might be measuring the frequency of the exchanged photons without being detected, but this will not give him any information on Alice's position: he may only succeed in ruining Alice and Bob's exchange.

V. CONCLUSION

In this paper, a scheme that employs entanglement and squeezing to achieve a higher accuracy in position measurements and distant clock synchronization has been analyzed in detail. In particular, the sensitivity to the loss has been addressed. A quantitative analysis of different strategies to contrast the loss has been presented. One finds that, even though the system is in principle very sensitive to the loss of a single photon, there are many situations where it may still be employed with an accuracy enhancement over the analogous classical schemes. It has been shown that relaxing the requirements of having maximally entangled states in frequency, one can achieve greater resistance to losses. A positioning quantum-cryptographic protocol has also been described. It allows only trusted parties (and no one else) to discover their relative positions.

An interesting feature, that has been analyzed elsewhere [17], is also present in our proposal. Namely, it is possible to exploit the robustness of the frequency entanglement when the pulses travel through dispersive media [13]. This may be used to achieve positioning and clock synchronization of distant parties without being affected by the intermediate dispersion that would distort any timing signal the parties exchange.

This work was funded by the ARDA, NRO, and by ARO under a MURI program.

-
- [1] C. H. Bennet, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
 - [2] C. M. Caves, Phys. Rev. D **23**, 1693 (1981); R. S. Bondurant and J. H. Shapiro, Phys. Rev. D **30**, 2548 (1984); B. Yurke, Phys. Rev. Lett. **56**, 1515 (1986); B. Yurke, S. L. McCall, and J. R. Klauder, Phys. Rev. A **33**, 4033 (1986); M. J. Holland and K. Burnett, Phys. Rev. Lett. **71**, 1355 (1993); J. P. Dowling, Phys. Rev. A **57**, 4736 (1998).
 - [3] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, Phys. Rev. A **54**, R4649 (1996).
 - [4] A. N. Boto, P. Kok, D. S. Abrams, S. L. Braunstein, C.

- P. Williams, and J. P. Dowling, Phys. Rev. Lett. **85**, 2733 (2000).
- [5] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
- [6] V. Giovannetti, S. Lloyd, and L. Maccone, Nature **412**, 417-418 (26 July 2001).
- [7] U. M. Titulaer, and R. J. Glauber, Phys. Rev. **140**, B676 (1965); U. M. Titulaer, and R. J. Glauber, Phys. Rev. **145**, 1041 (1966).
- [8] L. Mandel and E. Wolf *Optical coherence and quantum optics* (Cambridge Univ. press, Cambridge, 1995).
- [9] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer ac. publ., Dordrecht, 1993).
- [10] S. S. Schweber, *An introduction to relativistic quantum field theory*, Row, Peterson And Company (1961).
- [11] N. Margolus and L.B. Levitin, Physica D **120**, 188 (1998).
- [12] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
- [13] A. M. Steinberg, P. G. Kwiat, and R. Y. Chiao, Phys. Rev. A **45**, 6659 (1992); A. M. Steinberg, P. G. Kwiat, and R. Y. Chiao, Phys. Rev. Lett. **68**, 2421 (1992).
- [14] O. Pfister, W. J. Brown, M. D. Stenner, and D. J. Gauthier, Phys. Rev. Lett. **86**, 4512 (2001).
- [15] H. Carmichael, *An Open System Approach to Quantum Optics*, Springer-Verlag, Heidelberg (1993).
- [16] W. Dür, “Entanglement molecules”, Eprint quant-ph:/0006105.
- [17] V. Giovannetti, S. Lloyd, L. Maccone, and F. N. C. Wong, “Clock synchronization with dispersion cancellation”, Eprint quant-ph/0105156.